# Method and arrangement for watermark detection

## FIELD OF THE INVENTION

The invention relates to a method and arrangement for detecting a watermark in a media signal, more particularly in a media signal being played back through a graphics card of a personal computer.

## BACKGROUND OF THE INVENTION

Until very recently the DVD copy-protection community considered watermark-detection for playback-control in a personal computer to take place in the DVD-ROM or DVD-rewriter drive. The motivation for this position was that watermark-detection is a permissive technology (i.e. the playback or recording device works with or without watermark detector) as opposed to encryption, which requires a decryptor for the device to function properly. The fragile consensus used to be that DVD-ROM drives would inspect MPEG2-compressed unencrypted DVD-video content on disks for presence of a copy-never or copy-once watermark. If such were the case, playback should be stopped (because copy-once or copy-never content should be encrypted at all times).

Fig. 1 shows schematically such a PC system architecture with watermark-detection for playback-control in the DVD-drive. The PC comprises a DVD-drive 1, a motherboard 2 with microprocessor and associated circuitry for executing the operating system and application software, and a graphics card 3. The motherboard is provided with an IDE-bus 4 for transferring data to and from the DVD-drive, and an AGP-slot or PCI-slot 5 for connecting the graphics card. The DVD-drive includes a basic engine 11 for reading data from a DVD disk 6 and a host interface 12 for connecting the drive to the IDE bus. In order to enable watermark detection by a watermark detector core 14, the drive comprises an MPEG2-parser 13 to at least partially decompress the content. Stopping playback of content is symbolically denoted by means of a switch 15, which is controlled by the watermark detector core 14.

However, a PC system with playback-control using a watermark detector in the DVD drive leaves major security holes in an open-architecture PC. One such security hole is that content may be recorded in scrambled form by flipping all bits. Since this is no

longer a compliant MPEG2 stream, the parser 13 in the drive will fail and no watermark will be seen. The bit-flip can be undone just before or inside the media-player software. Another such security hole is that content may be compressed not using MPEG2, but using other compression schemes such as MPEG4 (popularized under the name DivX), fractal coding, Windows Media, Real, etc. Since it is impossible for the DVD-drive to have parsers on board for all of these formats (and hackers will invent new codecs to outsmart the drive), the watermark will not be detected. Although (illegal) copies compressed with a codec other than MPEG2 will generally not play on current DVD-video players there is a trend for DVD-video players to support more and more codecs.

Therefore it has already been proposed to place the watermark detector after decompression and just before rendering, i.e. in an MPEG-decoder card or in a graphics card. After decompression there is no longer confusion because all content reduces to the unequivocal baseband-format ready for consumption by human eyes. Initially, it was considered difficult to enforce MPEG-decoder companies or graphics-card manufacturers to install such watermark detectors. This perception has changed since.

Although it is architecturally very simple and clean to detect watermarks in the graphics-card, in practice there are a number of problems with this location, due to the enormous amounts of data that flow through the graphics card at huge speed, and due to the fact that multiple streams can be displayed at the same time.

## OBJECT AND SUMMARY OF THE INVENTION

It is an object of the invention to provide a solution for the above-identified problems. To this end, the invention provides methods and arrangements as defined in the independent claims. Advantageous embodiments are defined in the dependent claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows schematically a prior art personal computer architecture with watermark-detection in the DVD-drive.

Fig. 2 shows a computer system with a graphics card in accordance with one aspect of the invention.

Fig. 3 shows a computer system with a graphics card in accordance with a further aspect of the invention.

Figs. 4A and 4B show screen shots to illustrate the operation of the personal computer, which is shown in Fig. 3.

Fig. 5 shows a diagram of protocols carried out by the personal computer, which is shown in Figs. 2 and 3.

DESCRIPTION OF EMBODIMENTS

Fig. 2 shows a computer system with a graphics card 30 (connected to or integrated in the PC motherboard 2) in accordance with one aspect of the invention. The graphics card comprises conventional circuits such as an AGP/PCI interface 301, a display engine 302, a memory interface 303, a video RAM 304, and D/A convertors 305. A baseband watermark detector 31 is coupled to the output (or multiple outputs) of the graphics card, just before video data is applied to an (external) display screen. The watermark detector 31 controls one or more switches 35 to prevent content from being displayed on the display screen, in accordance with the applicable copy protection algorithm. The switches 35 have the same function as the switch 15 in Fig. 1.

One of the problems is that the data on the output(s) is in RGB format whereas most watermark-schemes work with the luminance channel. Conversion from the RGB format to luminance Y according to the well-known formula $(Y/0.587) \equiv 0.509\,R + G + 0.194\,B$ (where $0 \leq R,G,B < 1$) requires 2 additions and 2 multiplications. This is very costly, especially at high data rates.

In the system according to the invention, an RGB-to-Y converter 32 avoids multiplications by approximating Y, e.g. $Y \approx 0.25\,R + 0.5\,G + 0.125\,B = R/4 + G/2 + B/8$ which can be implemented with only arithmetic shifts. In an embodiment, which even prevents additions, the converter simply selects the green color signal so that $Y \approx G$ (because G is dominant).

Watermarks are often embedded by 'tiling' a small-sized basic watermark pattern over the entire image. The corresponding watermark detector divides the suspect image into image areas of the same size as the basic watermark pattern, accumulates said image areas in a buffer (a process referred to as folding), and checks the buffer for the presence of the basic watermark pattern in the accumulated image area. If the watermark detector 31 is of such a type, the 3 primary colors R,G,B are advantageously accumulated and folded first, using 3 separate fold-buffers. The conversion of RGB to Y is now performed off-line, after folding, instead of on-the-fly. This procedure takes 3 times more memory but that can usually be neglected with respect to the amounts of video-memory used for other purposes. This option requires more memory bandwidth though, because 3 times as much data must be transported to memory.

Another problem associated with the architecture, which is shown in Fig. 2, is that the video coming out of the graphics-card can be at any number of resolutions, as is illustrated in the following Table:

| Standard | Resolution | pixel-clock [MHz] |
|---|---|---|
| VGA | 640 × 480 | 27 |
| XGA | 1024 × 768 | 70 |
| SXGA | 1280 × 1024 | 116 |
| UXGA | 1600 × 1200 | 170 |

Table: Comparison of the resolutions and pixel-clock of some common graphics standards

There are other also other standards supported by some graphics cards, with interpolating resolutions. Note that the pixel-clock for normal baseband watermark detection (in PAL or NTSC) is 13.5 MHz. The output interface may thus have an up to 13× higher data rate (UXGA-mode) compared to normal PAL/NTSC baseband-detection. Baseband detection requires one addition for every pixel, so the adder has to work 13× faster.

To alleviate this problem, the graphics card includes a resolution converter 33, which sub-samples the pixel-data in space (and possibly also in time): e.g. the only information used for detection is line 1 from frame 1, line 2 from frame 2 etc. Alternatively, only a part of the images is being watermark detected.

Further, as shown in Fig. 2, there are multiple outputs on the graphics card. Currently, a computer (or its graphics card) is provided with a conventional VGA-output as well as a TV-output for displaying a DVD-movie rendered on the PC on a living-room TV. Recently the digital DVI-interface has been added to this palette. Because all these outputs can be controlled independently (i.e. display different data), naively the number of detectors should equal to the number of outputs, which constitutes a significant cost-burden.

This problem is solved by time-multiplexing the watermark detector onto the different outputs: i.e. first detect for a fixed amount of time on output 1, then on output 2 etc.. To this end, the system includes a selector 34, which time-sequentially selects one of the outputs of the graphics card. It is also possible to check all outputs simultaneously.

There are a number of further problems associated with detecting a watermark in the signal being generated by the graphics card of a personal computer. These further

problems are caused by the fact that a personal computer is generally able to simultaneously execute a plurality of applications in respective 'windows' of the display screen. Each window may often be arbitrarily positioned and scaled by the user.

The potential range of scales that the watermark detector 31 needs to deal with is thus very large. One of the highest scales still preserving visual quality is to display contents (e.g. a full-screen DVD-movie) on the monitor (blow up to 1600×1200 pixels or even more). Roughly the lowest scale is when the video is reduced to 352×200 pixels, which is a popular format for movies downloaded from the internet. The scale-range horizontally is thus 0.5...2.2 and vertically 0.4...2.5, whereas currently available watermark detectors are designed to deal with scales in the range 0.5...1.5.

In accordance with a second aspect of the invention, the video output of the computer is examined to locate image areas in which the signal changes from frame to frame. The video is thus distinguished from all the other information on the desktop, because real-time video contains many more changes. A bounding box is then generated around said image areas to provide a (preferably rectangular) area of interest. The bounding box is now considered to constitute the window in which the application runs.

Fig. 3 shows schematically a PC in accordance with this aspect of the invention. In this Figure, a pixel activity detector 36 detects and stores (thresholded) changes with respect to the previous frame. A joining circuit 37 fits a bounding box around image areas with significant change. It is well known from the literature how, starting from an area of activity one can determine the tightest possible bounding-box including such a point. Normal watermark detection is subsequently performed, where necessary preceded by scale conversion 32. In other words, whereas before (cf. Fig. 2) we had only scale detection and payload detection, we have now added "area-of-interest-detection".

To illustrate the operation of this PC architecture, Fig. 4A shows the desktop of a Microsoft Windows® operating system with two application windows 41 and 42, in which different applications are running. In this example, window 42 is generated by a DVD-movie player application. Fig. 4B shows the contents of the area-of-interest as detected by the circuitry (36, 37) in the graphics card. If the content in the area-of-interest is upsampled or downsampled to the normal 720×480 or 720×576 format, and supplied to a normal baseband watermark detector, it is very likely that the content is now processed at a scale sufficiently close to 1.0.

It should be noted that the change-detection 36 may be performed on a sub-sampled video-frame to conserve storage space. The change-detection may also be performed

"block-for-block" (e.g. first try to find the change-areas in the top-left corner, then in the top-right corner etc.).

A further aspect of the invention relates to acting on the detected presence or absence of the watermark. Fig. 5 shows schematically a diagram of protocols to make sure that all components are functioning ensure watermark detection.The blocks 16, 21, 22, and 38 denote authentication processes or devices. In this architecture being envisaged, the DVD-drive 10 checks, on boot-up, whether there is a graphics-card 30 with watermark detector 31 present in the PC. If such a graphics-card with watermark-detector is not present then the drive will not output data. If such a special graphics card is present however, it will output data.

When the watermark detector 31 in the graphics card detects a watermark it will try to authenticate to a compliant application which is responsible for rendering the watermarked data. If such authentication is successful, the graphics card continues operation (e.g. a valid DVD-Video is being played back using an authorized application). If it cannot find such a compliant application, the content must have come from some non-authorized source, e.g. an illegally copied disk in the drive is being rendered by some pirate or other non-compliant software. The graphics card will then shut down such output through activating the switches 35 (see Figs. 2 and 3), or otherwise destroy the viewing pleasure of the boxed area in which the watermark was detected. Alternatively, a message can be scrolled across the whole image to indicate the detection of a watermark in a non-authenticated stream.

The PC runs one or more applications, such as decompressing and rendering possibly watermarked contents obtained from a source such as DVD drive 10. Note that the compliant application is certain about the origins of the data which it is rendering because it has also authenticated with the drive. Note also that the architecture is more general. More particularly, the source is not necessarily a DVD-drive. For example, the source may also be an analog capture card, an MPEG-encoder card, or an IEEE-1394 board.

In the architectures shown above, a hacker may perform the following hack: (s)he copies illegal content which (s)he wants to watch from a DVD+R to the hard disk, without rendering. Then (s)he plays any valid protected DVD-video from the DVD-drive with a compliant application in one window, while the illegal material is rendered by a non-compliant application in another window. The watermark detector will find a watermark (in either one of the windows) but assume that to be consistent with the original movie in the DVD drive. Thus the illegal material is not caught. It is even possible to abuse a compliant

application: the illegal content on the hard disk can re-encrypted with CSS (which has been hacked), thus disguising it as valid content. This ReCSS-ed content is thus accepted by the compliant player, and after watermark detection in the graphics card, this application will vouch for it.

Therefore, when the detector has found watermarked content, which (through authentication) can be traced back to a compliant application or drive, the detector continues to search other areas-of-interest, and detect watermarks therein. In practice one could implement this by starting the bounding-box at a random point on the display, to avoid ending up with the same bounding-box all the time. If another watermarked area-of-interest is found, there must also be another compliant application or source. In the absence thereof, illegal contents is being played back, and the graphics card is controlled to act accordingly.

As an alternative the graphics card may notify the drive of the watermark-payload using the authenticated channel set up at boot-time. The drive can verify from the disk whether this watermark-payload is commensurate with this disk. If not, some other source of copied material must exist. Note that for this method to work, the watermark-payload needs to be stored on the disk in a manner that it cannot be retrieved by a hacker, e.g. in some currently unused sector in the lead-in area. This does not add cost to the drive.

A hacker may perform the following hack: he inserts a second non-compliant graphics card into the PC. He allows the drive to authenticate to the graphics card (using a hacked driver), while he uses the non-compliant card to playback illegal material from the drive. A second hack scenario is when he only inserts a non-compliant graphics card into his PC but connects the PC via a network (home network or internet) to another PC with a compliant graphics card. After authenticating the drive with the remote compliant graphics-card, illegal content is displayed on the on-board non-compliant graphics card. A third hack scenario is where there is a compliant DVD-drive and a compliant graphics card with watermark detector in a single PC: after authentication the hacker streams the data from illegal disk in the drive to a non-compliant application running on another PC with a non-compliant graphics card somewhere in the network.

The operating system and the BIOS are the only entities in the PC which have reliable knowledge about the plug-in card configuration of the PC. A solution for the first hack-scenario is for the BIOS or OS to prohibit combinations of compliant and non-compliant graphics cards in a PC (for security reasons). A solution for the second hack-scenario is for OS and BIOS to disallow authentication with graphics cards across the network. A way to implement this would be for the OS to query the drive which graphics

card it authenticated with and to check that the device is indeed on board. This obviously requires a secure OS. If it is a market requirement that playback from a remote DVD-drive in a home network should be allowed, the second scenario hack of problem 7 cannot be prevented. Another solution is for the OS to prohibit combinations of compliant drive and non-compliant graphics card in the same box.

The invention may be summarized as follows. Watermark-detection in the graphics card of a personal computer, for the purpose of copy-protection, has recently started to draw a lot of attention in standardization. Detection in the graphics card has problems completely different from the formerly considered detection in the DVD-drive, having to do with high data-rates, large scale-ranges and presence of multiple video-streams in the display area. This invention proposes conversion (32) of the computer's RGB output into a luminance signal (Y) prior to watermark detection by a conventional watermark detector (31) being arranged to detect the watermark in a such a luminance signal. The resolution of the monitor image to be inspected is preferably converted (33) to the conventional TV resolution of the (MPEG2-compressed) contents being played back on the computer's DVD drive. In graphic cards providing multiple outputs (VGA, TV, DVI), the same watermark detector may be time-sequentiall connected (34) to each of the outputs.